Cassandra Crossing/ IoT: temere il vecchio od il nuovo?

(616)—Per essere sicuri, dicono, è necessario gettare i vecchi oggetti IoT e sostituirli con altri nuovi. Ma bisogna temere di più i…

Cassandra Crossing/ IoT: temere il vecchio od il nuovo?



Figure 1:

(616)—Per essere sicuri, dicono, è necessario gettare i vecchi oggetti IoT e sostituirli con altri nuovi. Ma bisogna temere di più i nuovi od i vecchi?

16 aprile 2025—Non solo i 24 informatissimi lettori di Cassandra, ma chiunque si abbeveri, anche se di rado, alle notizie tecnologiche disponibili in Rete e fuori, si sarà imbattuto negli allarmi contro le "cose" informatiche vecchie, in particolare gli oggetti dell'IoT.

Questi articoli grondano di saggezza e buone intenzioni, ed eccone qui un esempio recentissimo. che mette in guardia dagli oggetti IoT non più aggiornabili.

Dice solo cose giuste. Come dargli torto!

Al pari di tutti gli hardware ed i software ordinari, i "vecchi" oggetti IoT, contengono certamente numerosi bug, magari anche a livello di progetto.

I Nabaztag di Cassandra hanno firmware abbandonati rispettivamente dal 2005, 2007 e 2010, connessioni parzialmente in chiaro, alcuni non hanno nemmeno CPU ma microcontrollori; non c'è insomma nessuna possibilità che siano sicuri.

Ah, non sapete cosa sia un Nabaztag? A voi una chiacchierata sull'argomento ed un intero corso.

Eppure questi Nabaztag stanno online nella loro rete locale, senza che Cassandra sia impazzita od abbia sgarrato ai suoi stessi precetti. Come è possibile? Intanto proseguiamo; ci torneremo sopra.

Quello che abbiamo detto dei Nabaztag vale anche per qualsiasi altro oggetto sia attaccato alla nostra rete locale (a cominciare dal modem) o direttamente “a noi” (smartphone, orologio, braccialetto fitness).

Qualsiasi oggetto il cui firmware non venga aggiornato periodicamente, meglio se in automatico, è potenzialmente più attaccabile di uno che si aggiorni. Un firmware vecchio di due anni o più è un chiaro segno di un oggetto “abbandonato” dal fabbricante. Si deve buttare un oggetto IoT “abbandonato” per timore che venga attaccato ed usato come ponte per entrare nella nostra rete? Non necessariamente, solo come caso estremo, e vedremo perché.

Si deve senz’altro buttare, od almeno spegnere o scollegare, qualsiasi oggetto connesso che non sia più utile al proprietario. Fosse anche sicurissimo, per il solo fatto di esistere ed essere connesso costituisce comunque un pericolo.

Infatti, l’unico oggetto IoT sicuro è quello che non esiste. Anche un oggetto IoT spento e scollegato tuttavia potrebbe sempre cadervi in testa!

Se un oggetto IoT è vecchio, e non ci accontentiamo di tenerlo come soprammobile inerte, ma lo vogliamo mantenere connesso, è necessario quantomeno isolarlo dalla rete e da tutti gli altri oggetti IoT in nostro possesso. Qui non è possibile dare istruzioni generali, ma la maggior parte dei router casalinghi moderni permettono di fare una od ambedue queste cose.

1—realizzare una seconda rete wifi o cablata separata da quella principale, che non può parlare con quest’ultima, e che non permette nemmeno agli oggetti collegati di parlare tra loro, ma solo di connettersi ad Internet;

2- isolare un singolo oggetto in modo che possa solo connettersi ad internet ma non scambiare dati in locale, oppure possa comunicare solo con un altro determinato oggetto della rete locale.

Utilizzando queste due funzioni, bisogna segregare gli oggetti IoT non più aggiornati, in modo tale che non possano comunicare con gli oggetti più recenti e “sani”, ma solo con quelli strettamente necessari.

Ad esempio, una presa di corrente “intelligente” deve comunicare solo con il server di domotica tipo Home Assistant, ma non con gli altri oggetti IoT, e nemmeno essere in grado di connettersi ad Internet.

Ci vuole tempo e sbattimento. Si, ma nemmeno tanto, ed è comunque utile al fine di prendere conoscenza della nostra vita digitale vera.

Bene, fermiamoci qui per gli oggetti IoT “vecchi”. **E quelli appena comprati, invece?**

Qui il problema, o meglio il pericolo, cambia completamente, come pure i “cattivi” da cui guardarsi.

E’ pur vero che anche gli oggetti IoT “nuovi” possono avere dei bug ma, se attivamente aggiornati, abbiamo almeno la speranza che ci sia qualcuno, da qualche parte, pagato per tutelare anche la nostra sicurezza tramite la correzione dei bug e l’aggiornamento automatico del firmware. Controlliamo ogni oggetto in casa e, se è così, possiamo stare un po’ più tranquilli.

Il pericolo, o meglio la certezza, di essere fregati viene stavolta da chi ha già preso i nostri soldi, cioè dal **fabbricante dell’oggetto**.

La regola è che **se un oggetto IoT è recente, contiene certamente funzionalità non necessarie, che sono realizzate per trasmettere alcuni vostri dati personali al fabbricante, al fine di elaborarli e rivenderli**.

Se non ci credete, o sottostimate l'entità e l'onnipresenza di questo problema, siete caldamente invitati a leggere, ad esempio, questo articolo che riguarda voi, la vostra Smart-TV e l'ACR. Cos'é l'ACR? Appunto, leggete l'articolo!

Se non vi convincete nemmeno così perché tanto *non avete niente da nascondere*, mi dispiace. Cassandra non è certamente una lettura adatta a voi.

Cosa fare dunque? Purtroppo i mezzi per eliminare o limitare questo tipo di danno sono pochi.

Fare a meno dell'oggetto, cosa che fa anche risparmiare, oppure se possibile impedire che si connetta ad Internet (per una presa intelligente probabilmente lo potete fare), oppure **limitare i dati che può catturare**.

Ad esempio, ad una Smart-TV potete disabilitare l'ACR e le altre funzionalità di profilazione disabilitabili, e successivamente, con l'ausilio di un firewall, permetterle di connettersi ai soli ai server di streaming tipo Netflix, bloccando tutte le altre connessioni, od almeno quelle ai server ACR del fabbricante.

Sono cose difficili? Non sono semplici, ma se volete sopravvivere nel mondo digitale, e non ridurvi ad Eloi e cibo per i Morlock, lo dovete fare. Dovete seguire l'eterno e sempre valido ammonimento di V.

Vi sentite smarriti? E magari i continui e ripetitivi ammonimenti di Cassandra vi hanno stancato?

Guardatevi attorno; non siete soli, ci sono persone ed associazioni che vi possono aiutare, di persona o fornendovi informazioni o, come fa nel suo piccolo Cassandra, anche solo ammonendovi e spronandovi.

Ma dovete metterci del vostro, altrimenti non avrete scampo.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

Licenza d'utilizzo*: i contenuti di questo articolo, sono sotto licenza Creative Commons Attribuzione—Condividi allo stesso modo 4.0 Internazionale (CC BY-SA 4.0),* tutte le informazioni di utilizzo del materiale sono disponibili a questo link.

By Marco A. L. Calamari on April 16, 2025.

Canonical link

Exported from Medium on August 27, 2025.